Trabalho - II
MO422 – Algoritmos Criptográficos
Prof. Ricardo Dahab

1 Introdução

O trabalho consiste no estudo e implementação de um algoritmo simétrico de encriptação ou de um algoritmo para o cálculo de resumos criptográficos (hash). Deverão ser entregues um trabalho escrito e um arquivo com o programa fonte da sua impelementação, em linguagem à sua escolha.

2 Algoritmos

Encriptação

O algoritmo para seu trabalho é de sua escolha, mas deve ser um dos algoritmos "leves", isto é, de baixo consumo de recursos, constantes no seguinte website:

`https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers`

Resumos criptográficos

Igualmente, para o caso de resumos, o website com os algoritmos a serem estudados é o seguinte:

`https://www.cryptolux.org/index.php/Lightweight_Hash_Functions`

3 Formato do trabalho escrito

O trabalho escrito deve ter a seguinte estrutura:

```
1. Resumo do trabalho
2. Descrição do algoritmo
   2.1 Autores
   2.2 Descrição em alto nivel
   2.3 Descrição dos detalhes do algoritmo
   2.4 Desempenho observado e medido, inclusive em comparação
```

```
      com outros para o mesmo fim.
   2.5 Histórico do algoritmo: participação em chamadas
      públicas, ataques, etc.
3. Implementações de referência:
   3.1 Quais e onde estão.
   3.2 Breve comparação dos tempos de execução do seu
      código e de uma implementação de referência.
```

4 Sobre a implementação a ser entregue

Sua implementação deve estar correta e entregue na forma de um arquivo com o programa fonte, na linguagem de sua escolha. Se você tiver tempo de disponibilizá-lo para execução em algum website, isto é melhor ainda mas não é obrigatório.

Além do arquivo com o código-fonte, você deve disponibilizar no mesmo diretório exemplos de execução do seu algoritmo. Não é necessário seguir nenhum padrão de formatação dos dados de entrada.

5 Data de entrega

A data final de entrega é 16 de dezembro.

6 Instruções adicionais

Aqui estão algumas instruções posteriores à postagem inicial:

- **25/11.**
  - Alunos de graduação podem fazer o trabalho em duplas. Alunos de pós-graduação devem fazer individualmente.
  - O trabalho escrito deve conter de 15 a 20 páginas, tamanho A4, fonte tamanho 11.
  - Na descrição em alto nível do algoritmo (seção 2.2), você deve deixar claro o critério de projeto seguido pelo algoritmo (p. ex., redes de Feistel (encriptação), esponja (hash), etc.)